STATE OF CALIFORNIA DMV DEPARTMENT OF MOTOR VEHICLES

A Public Service Agency

BONDED WEB USER PROGRAM
INFORMATION SECURITY PRE-IMPLEMENTATION CHECKLIST

BONDED WEB USER NAME	TELEPHONE NUMBER ( )

BUSINESS ADDRESS	CITY	STATE	ZIP CODE

USE THE NUMBER LISTED BELOW TO IDENTIFY THE NARRATIVE, DIAGRAM, FLOOR PLAN, OR SUBMITTED MATERIAL WHEN PUTTING YOUR PACKAGE TOGETHER. *Place this form on top of the completed package.*

To assure a secure environment is maintained, DMV requires that administrative measures and minimum standards are met by the Bonded Web User. To ensure that DMV measures and standards are met prior to implementation the users must provide the following information or documents:

GENERAL SECURITY INFORMATION

□ 1. Provide a copy of each of the following:

- The security policies and/or information security program policies pertinent to the Bonded Web User Program;
- The user guide or processing manual for registration transactions and controlling inventory; and
- The guidelines or training manual(s) for physical and electronic access for your staff authorized to work with DMV resources and assets.

□ 2. Provide a description of the Bonded Web User process(es) for identifying possible security incidents. Identify what procedures or process(es) are utilized to prevent further security violation(s) after they are found, and how a security violation is documented and reported to DMV.

RESOURCE AND ASSET PHYSICAL SECURITY

□ 3. Provide a floor plan and a detailed narrative describing workstation and facility security. The documentation must include overall facility security and intrusion prevention, entry control measures, as well as details regarding the area(s) where DMV resources and assets are used, or stored (permanent and working storage), and where electronic data manager workstations and printers are located. Include details regarding security control measures (i.e., the location and descriptions of any safe(s) or file cabinet(s) used for DMV controlled and accountable items security; identify areas that are public and employee and authorized employees only; details regarding facility security measures (i.e., alarm or surveillance systems); and identify the locations of internal and external doors, window, and other openings and how they are secured).

ACCESS SECURITY

□ 4. Provide a narrative that details how users are IDENTIFIED, AUTHENTICATED, and AUTHORIZED access to DMV Bonded Web User processes, resources, and assets.

COMPUTER SYSTEM AND OR NETWORK SECURITY

□ 5. Provide a detailed narrative and diagram that describes the Bonded Web Users' network and or system, including the Bonded Web User DMV interface. Please state the logical security measures and methods utilized to secure the network and or system.

RETENTION AND DESTRUCTION SECURITY

□ 6. Provide a narrative that details how DMV information resources are secured and kept private while retained or captured via any method and/or medium (electronic or physical), fixed or portable.

□ 7. Provide a narrative that details how DMV information resources and assets are rendered unreadable, unusable, and unrecoverable after legitimate business use has ended or destruction is required.

DECLARATION STATEMENT

I certify (or declare) under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

As the Authorized or Designated representative of: ______________________________
BUSINESS NAME

PRINTED NAME OF AUTHORIZED REPRESENTATIVE

SIGNATURE OF AUTHORIZED REPRESENTATIVE X	DATE

Print   Clear Form